Configurer un profil de cryptage et terminer la configuration du compte RES pour ESA

Introduction

Ce document décrit comment créer un profil de cryptage et provisionner un compte Cisco Registered Envelope Service (CRES) pour un Cisco ESA.

Remarque : Il existe des différences entre l'appliance de sécurité de la messagerie électronique virtuelle/hébergée (ESA) et l'ESA matérielle. Passez en revue les sections appropriées pour votre type de déploiement.

Cet article explique également comment résoudre le problème « Impossible de provisionner le profil <profile_name> pour la raison suivante : Erreur « compte introuvable », fréquemment rencontrée sur les modèles ESA virtuels et hébergés lors de l'ajout d'un profil de chiffrement. Si cette erreur s'affiche, suivez les étapes de la section ESA virtuel et hébergé.

Conditions préalables

Exigences

- Assurez-vous que la clé de fonction IronPort Email Encryption est installée sur votre ESA.
- Pour le vérifier, utilisez l'interface graphique utilisateur ESA dans Administration système > Touches de fonction ou exécutez feature key sur l'interface de ligne de commande ESA.

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configuration du profil de provisionnement et de chiffrement des

comptes

Provisionnement du compte CRES pour les ESA virtuels et hébergés

Les appliances ESA virtuelles et hébergées peuvent afficher l'erreur « Unable to provision profile <profile_name> for reason: Impossible de trouver le compte lors de l'approvisionnement d'un profil de chiffrement :



Cisco doit compléter le compte de mise en service CRES pour vous. Ouvrez un dossier Cisco TAC avec ce qui suit :

- Nom du compte (indiquez le nom exact de la société tel qu'il doit apparaître).
  - Pour les comptes hébergés, terminez le nom du compte par <Nom du compte> HOSTED.
- Adresse(s) e-mail de l'administrateur du compte (indiquez son adresse e-mail).
- Le ou les numéros de série complets du ou des SEEE concernés.
  - Procurez-vous le numéro de série à partir de System Administration > Feature Keys dans l'interface utilisateur graphique ou utilisez la version sur l'interface de ligne de commande.
- Domaines à mapper au compte CRES pour l'administration.

Remarque : Si un compte CRES existe déjà, indiquez le nom de la société ou le numéro de compte CRES utilisé précédemment. Cela permet de s'assurer que les nouvelles appliances sont ajoutées au compte approprié et d'éviter les doublons.

Remarque : Un numéro de série ne peut être enregistré que sur un seul compte dans CRES.

Plusieurs appliances peuvent être enregistrées sur un même compte CRES.

Si vous avez déjà essayé de créer le profil de cryptage sur l'ESA, procédez comme suit :

1. Accédez à Security Services > Cisco IronPort Email Encryption > Email Encryption Profiles dans l'interface graphique utilisateur ESA.
2. Sélectionnez Re-provision. L'état du profil passe à Provisionné en cas de réussite.
3. En cas d'échec, poursuivez les étapes de création de profil pour votre modèle ESA.

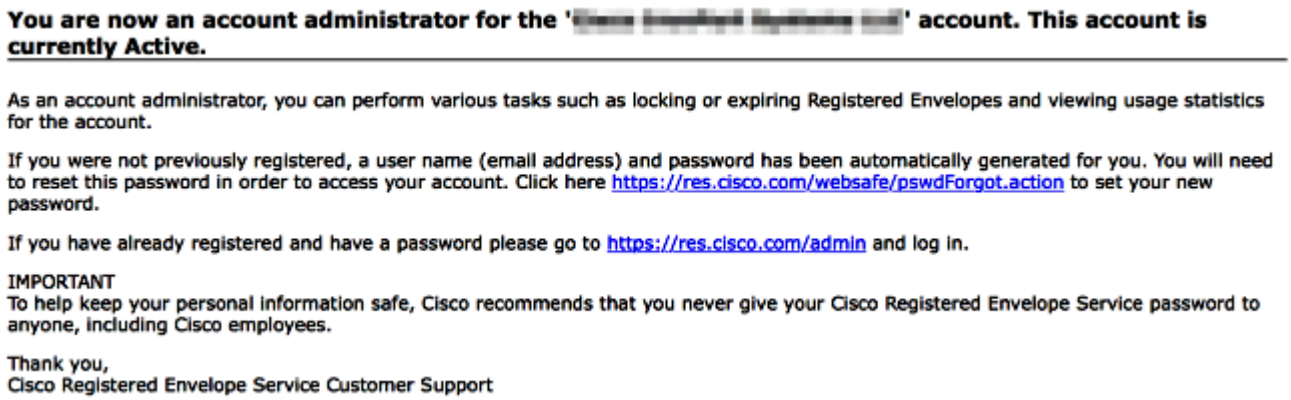
Provisionner le compte CRES pour le matériel ESA

Les ESA matériels, à partir de la version 4.2 de CRES, peuvent provisionner automatiquement et ne nécessitent pas la création manuelle de comptes par e-mail.

1. Dans l'interface graphique utilisateur ESA, accédez à Security Services > Cisco IronPort Email Encryption, activez la fonction, puis acceptez le contrat de licence de l'utilisateur final (CLUF) si ce n'est pas déjà fait.
2. Sélectionnez Modifier les paramètres.
3. Saisissez l'adresse e-mail de l'administrateur dans le champ Adresse e-mail de l'administrateur du compte de cryptage et sélectionnez Envoyer.
4. Créez un profil de chiffrement à l'aide du bouton Ajouter un profil de chiffrement.
5. Lors de la création d'un profil, spécifiez un nom de profil significatif pour référence dans les filtres de messages ou de contenu.
6. Sélectionnez Envoyer.
7. Le nouveau profil s'affiche comme Non provisionné. Validez vos modifications avant de continuer.
8. Après avoir validé les modifications, sélectionnez Provisionner pour terminer le processus de provisionnement.
9. Une fois le provisionnement terminé, une bannière apparaît et le bouton de provisionnement du profil devient Re-provisioning.
10. La configuration du profil de chiffrement est maintenant terminée. Vous pouvez chiffrer le courrier de vos appareils via CRES.

Notification et vérification de l'administrateur du compte

Vérifiez votre configuration en vérifiant que l'adresse e-mail de l'administrateur reçoit une notification du statut de l'administrateur du compte :



You are now an account administrator for the '[redacted]' account. This account is currently Active.

As an account administrator, you can perform various tasks such as locking or expiring Registered Envelopes and viewing usage statistics for the account.

If you were not previously registered, a user name (email address) and password has been automatically generated for you. You will need to reset this password in order to access your account. Click here https://res.cisco.com/websafe/pswdForgot.action to set your new password.

If you have already registered and have a password please go to https://res.cisco.com/admin and log in.

IMPORTANT
To help keep your personal information safe, Cisco recommends that you never give your Cisco Registered Envelope Service password to anyone, including Cisco employees.

Thank you,
Cisco Registered Envelope Service Customer Support

Après avoir reçu cette notification, connectez-vous au site CRES Admin et vérifiez votre compte. Le numéro de compte apparaît dans le récapitulatif du compte. Pour garantir une visibilité complète de tous les domaines enregistrés, ouvrez un dossier Cisco TAC avec :

- Numéro de compte
- Nom du compte
- Domaines à mapper pour l'administration

Cela garantit que votre compte a un accès complet à tous les domaines enregistrés via CRES.

Détails du numéro de compte CRES

Le numéro de compte CRES est basé sur les informations de contrat liées à l'appliance, générées à partir de l'ID GU (Global Ultimate), et le nom du compte est basé sur le nom du site d'installation. Pour les vérifications de vérification et d'autorisation, utilisez le Centre de contrats de service Cisco (CSCC).

Dépannage

Cette section décrit les étapes à suivre pour vérifier la connectivité ESA aux serveurs CRES.

Pour vérifier la connectivité, utilisez cette commande sur l'interface de ligne de commande ESA :

<#root>

```
esa.example.com>

telnet res.cisco.com 443

Trying 10.94.241.74...
Connected to 10.94.241.74.
```

```
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Cette commande vérifie si l'ESA peut atteindre le serveur CRES sur le port 443. Utilisez-la uniquement pour la vérification de connectivité ; ne pas utiliser pour d'autres étapes de dépannage.

Informations connexes

- Guides d'utilisation de l'appliance de sécurisation de la messagerie Cisco
- Ressources d'assistance technique et de documentation Cisco
- Identifier les adresses IP et les noms d'hôte du serveur de clés Cisco RES
- Définir un logo personnalisé dans CRES

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.